CLAIMS

What is claimed:

1. A method for determining unauthorized network usage, comprising the steps of:

capturing packet header information from communications on a network;

determining valid connections or data flows;

determining hosts on the network that act as a client and server for each valid connection or data flow; and

determining network services being used by every host in a predefined group of hosts.

2. The method of claim 1, further comprising the step of displaying indicia indicating observed network services during a monitoring period.

3. The method of claim 2, further comprising the step of displaying an indication of the observed network services which were previously seen during the presentment period.

4. The method of claim 1, further comprising the steps of:

storing an allowed network services profile;

comparing allowed network services with observed network services; and

generating an alarm when an observed network service is not an allowed network service.

5. The method of claim 3, further comprising the step of displaying indicia indicating whether the observed network services is not an allowed network service.

6. The method of claim 4, further comprising the step of building a network service profile based upon network services observed during a profile generation time period.

7. The method of claim 4, further comprising editing the allowed network services profile.

8. The method of claim 4, further comprising the step of editing the allowed network services profile for a block of network address.

9. A method for determining unauthorized network usage, comprising the steps of:

capturing packet header information from communications on a network;

determining hosts on the network that act as a client and server for each valid connection or data flow;

determining network services being used by every host in a predefined group of hosts; and

generating an alarm upon an observed network service not being included in a, allowed network service profile.

10. A method for determining unauthorized network usage, comprising the steps of:

capturing packet header information from communications on a network;

determining valid connections or data flows;

storing an allowed network service port profile for each in a predefined host group;

determining observed network service port numbers being used by every host in the predefined host group for each valid connection or data flow;

comparing the allowed network service port profile with observed network service port numbers; and

generating an alarm when an the observed network service port number is not included in the allowed network service port profile.

11. The method of claim 10, further comprising the step of displaying indicia indicating the observed network service port numbers during a present monitoring period.

12. The method of claim 11, further comprising the step of displaying an indication of the observed network service port numbers which were previously seen during the presentment period.

13. The method of claim 12, further comprising the step of displaying indicia indicating whether the observed network service port numbers is included in the allowed network service port profile.

14. The method of claim 10, further comprising the step of building the network service port profile based upon the observed network service ports observed during a profile generation time period.

15. The method of claim 10, further comprising editing the allowed network service port profile.

16. The method of claim 15, further comprising the step of editing the allowed network service port profile for a block of network addresses.

17. A system for determining unauthorized network usage, comprising:

a monitoring device operable to observe communication packets on a network;

a computer system operable to capture packet header information from observed communication packets;

the computer system operable to determine valid connections or data flows;

the computer system operable to determine hosts on the network that act as a client and server for each valid connection or data flow; and

the computer system operable to determine network services being used; and

the computer system operable to generate an alarm when an observed network service is not an allowed network service.

18. The system of claim 17, further comprising a monitor coupled to the computer system operable to display indicia indicating observed network services during a monitoring period.

19. The system of claim 18, further comprising the monitor operable to display indicia indicating whether the observed network services is not an allowed network service.

20. The system of claim 17, further comprising the computer system operable to build a network service profile based upon network services observed during a profile generation time period.

21. The system of claim 17, further comprising an editor couple to the computer system operable to edit the allowed network services profile.

22. The system of claim 21, further comprising the editor operable to edit the allowed network services profile for a block of network address.